

SANDIA REPORT

SAND201X-XXXX

Unlimited Release

Printed Month and Year

The Cyber Defense (CyDef) Model for Assessing Countermeasure Capabilities

Margot Kimura, Troy DeVries, and Susanna Gordon

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.



Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: <http://www.osti.gov/scitech>

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: <http://www.ntis.gov/search>



The Cyber Defense (CyDef) Model for Assessing Countermeasure Capabilities

Margot Kimura¹, Troy DeVries², and Susanna Gordon³

¹Cyber Systems Assessments (08766)

²Enterprise Cyber Security (08765)

³Systems Research & Analysis III (08716)

Sandia National Laboratories
P. O. Box 969
Livermore, California 94551-0969

Abstract

Cybersecurity is essential to maintaining operations, and is now a de facto cost of business. Despite this, there is little consensus on how to systematically make decisions about cyber countermeasures investments. Identifying gaps and determining the expected return on investment (ROI) of adding a new cybersecurity countermeasure is frequently a hand-waving exercise at best. Worse, cybersecurity nomenclature is murky and frequently over-loaded, which further complicates issues by inhibiting clear communication.

This paper presents a series of foundational models and nomenclature for discussing cybersecurity countermeasures, and then introduces the Cyber Defense (CyDef) model, which provides a systematic and intuitive way for decision-makers to effectively communicate with operations and device experts.

ACKNOWLEDGMENTS

Thank you to Samuel Kane and Andreina Ray, who helped with developing some of the diagrams.

Thank you also to the many folks who provided helpful conversations in the course of developing these models and nomenclature, including Heidi Ammerlahn, Jeff Boote, Denise Grayson, CW Perr, Levi Lloyd, Karim Mahrous, and Noel Nachtigal.

TABLE OF CONTENTS

1.	Introduction.....	9
1.1.	Purpose.....	9
1.2.	Scope.....	9
1.3.	Organization.....	9
2.	Foundational Models	11
2.1.	The Elements of Cyber Defense	11
2.1.1.	Prevention	11
2.1.2.	Detection	11
2.1.3.	Response	11
2.2.	Locations.....	12
2.2.1.	Host	12
2.2.2.	Intranet	12
2.2.3.	Border.....	13
2.2.4.	Cloud, Mobile, and Internet of Things.....	13
2.2.5.	Notes on the “Best” Location.....	13
2.3.	Countermeasure (CM) Nomenclature.....	15
2.3.1.	Actions by Defense Element.....	15
2.3.2.	Prevention Action Rules	19
2.3.3.	Variations on Applying Actions	19
3.	Cyber Defense Model Components.....	21
3.1.	Cyber Attack Phases (CAPs)	21
3.2.	The Pain Scale.....	22
3.3.	Coverage Metric.....	23
4.	The Cyber Defense (CyDef) Model.....	25
4.1.	The CyDef Chart as a Decision Aid	26
4.1.1.	Example: CM Investment Decision	26
5.	Conclusions & Next Steps	29
6.	References.....	31

FIGURES

Figure 1: Physical security analogy for the elements of cyber defense.....	11
Figure 2: General categories of locations that are relevant to the CyDef Model.	12
Figure 3: The Cyber Attack Phases (CAP), which shows an attacker's general workflow in terms of a series of steps that a defender can potentially inhibit.	21
Figure 4: Coverage Metric.....	23
Figure 5: Conceptual diagram for the Coverage Metric	24
Figure 6: An example CyDef chart for packet filtering, a very common CM.....	25
Figure 7: The CyDef chart, which displays a CM's applicable CAPs, with Pain and Coverage scores for each CAP.	26
Figure 8: CyDef chart an example decision.	27

TABLES

Table 1: Countermeasure Actions and Definitions	17
Table 2: Countermeasure Actions and Definitions, continued.	18
Table 3: The Pain Scale	23

ACRONYMS

Abbreviation	Definition
C2	Command & Control
CAP	Cyber Attack Phase
CM	Countermeasure
CyDef	Cyber Defense [Model]
IP	Internet Protocol
ISP	Internet Service Provider
PII	Personally identifiable information
ROI	Return on investment

This page is intentionally left blank.

1. INTRODUCTION

Cybersecurity is essential to maintaining operations, and is now a de facto cost of business. Despite this, there is little consensus on how to systematically make decisions about cyber countermeasures investments. Identifying gaps and determining the expected return on investment (ROI) of adding a new cybersecurity countermeasure is frequently a hand-waving exercise at best. Worse, cybersecurity nomenclature is murky and frequently over-loaded, which further complicates issues by inhibiting clear communication.

1.1. Purpose

The purpose of the Cyber Defense (CyDef) Model is to provide decision-makers, operations experts, security researchers, and device experts with a common model and set of nomenclature to strategically discuss and systematically prioritize options for cybersecurity countermeasures.

1.2. Scope

This initial version of the CyDef Model focuses on the case where a potentially large and multi-site organization wishes to strategically invest in cybersecurity countermeasures for its internal infrastructure. Cloud-computing, mobile devices, and internet-of-things devices are out of scope. While we expect the CyDef Model to be applicable to these areas, additional work is required to ensure that the nuances of those use cases are adequately addressed.

1.3. Organization

We begin by presenting a series of foundational models and nomenclature for discussing cybersecurity countermeasures. After establishing a common language and basis of understanding, we then introduce the CyDef model, which provides a systematic and intuitive way for decision-makers to effectively communicate with and make decisions with input from operations, device, and security experts. We provide an example of how the CyDef Model can be used to aid in making investment decisions, and then conclude with a brief summary of the model and notes on future development work to make the CyDef Model more operations-focused.

This page is intentionally left blank.

2. FOUNDATIONAL MODELS

This section establishes the foundational models and nomenclature underlying the Cyber Defense (CyDef) Model.

2.1. The Elements of Cyber Defense

We divide the broad needs of “cyber defense” into three main elements: prevention, detection, and response. All three elements are essential for an effective cyber defense system.

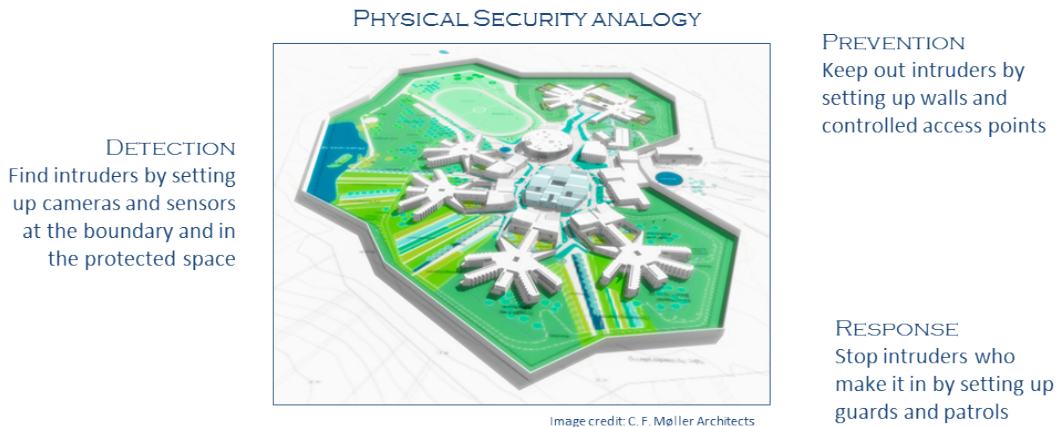


Figure 1: Physical security analogy for the elements of cyber defense.

2.1.1. Prevention

This element focuses on preventing threats from accessing the network in real time, using automated defenses in a smart network architecture. Prevention is relatively quick and inexpensive compared to detecting and responding to threats that have successfully penetrated systems. Thus, an effective defense works to defeat as much of the threat space as possible through increasingly effective prevention, thereby freeing resources to address only the most sophisticated threats via post-intrusion detection and response.

2.1.2. Detection

This element focuses on identifying threats so that they can be addressed via prevention or response measures. As of today, detection for prevention is signature based, whereas detection that supports response measures includes reactive monitoring and passive hunting, as well as information collection to drive those two main activities. Threats evolve quickly, so investing in sophisticated detection methods such as behavioral analytics can help identify new threat vectors for which up-to-date indicators can then be produced for preventative elements.

2.1.3. Response

This element focuses on responding to threats that have bypassed prevention elements and have penetrated systems. Incident response includes scoping (e.g., finding all entry points and affected machines), remediation, elevated monitoring, mitigation, and eradication. Incident response is

vital for stopping adversaries, mitigating and remediating damage, and preventing future incidents.

2.2. Locations

A countermeasure (CM) can provide different benefits, depending on where it is deployed: at the host, intranet, or border. When making investment decisions, it is important to understand which location is most appropriate for each type of defense element and CM.

Each subsection below provides a brief description of the location, its strengths, and its limitations.

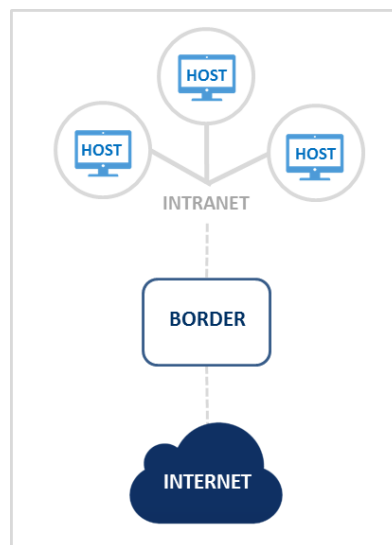


Figure 2: General categories of locations that are relevant to the CyDef Model.

2.2.1. Host

A “host” is an individual computer or computing resource within the organization’s internal network. An adversary’s goal typically involves manipulating one or more hosts, because this is where information is stored, accessed, and modified. Defenders can typically get the highest-fidelity information on what an adversary is doing by detecting and analyzing affected hosts.

Scaling issues typically prevent cyber defenders from closely monitoring hosts directly (i.e., the number of hosts is huge compared to the number of cyber defenders). In addition, hosts typically have the greatest interaction with sensitive information, including personally identifiable information (PII), and proprietary information, so caution is necessary when analyzing and monitoring hosts.

2.2.2. Intranet

The “intranet” refers to the internal network of an organization. The exact architecture will vary across organizations, but intranets are generally composed of a series of interconnected routers with clusters of hosts connected to each router. Network defenses deployed at this level analyze

the traffic that goes by in those internal routers, and are generally capable of identifying hosts associated with traffic. This location is generally the best for detecting lateral movement, in which an adversary tries to expand its access to the network (see Section 2.3), because sensors located in the intranet can analyze internal traffic that does not go out to the internet.

Scale is also an issue at this level, given the sheer number of attacks experienced by the typical externally-facing organization. This can be mitigated somewhat by deploying CMs at both the host and border levels, to reduce the scope of activities that would need to be monitored at the intranet level.

2.2.3. *Border*

A relatively common prevention practice is to reduce the number of connections out to the internet to a small number of monitored paths, and then to guard those connections with CMs. CMs located at the border must be able to process traffic at the velocity and volume that data is entering and leaving the organization's entire network. In other words, defenses deployed at this location have high requirements on throughput and availability. In addition, CMs placed at the border are not capable of detecting adversary movement or activity within the network, so these do not obviate the need for host and/or intranet CMs.

This vantage point provides the broadest system-wide vantage point for preventing attacks and establishing situational awareness. It is also a good "first defense" location for preventing known inbound attacks, because it can potentially remove attacks before they ever hit the network and help defenders drastically reduce the volume of traffic they need to analyze.

For detection, there is a fine distinction between placing a sensor either just outside or just inside the border defined by the location of the CMs. Outside the border, a sensor can see everything directed towards the organization, and potentially detect scans and attack attempts. However, the incoming data will be very noisy – it will be difficult to discern which traffic is malicious and which is not. Inside the border, the sensor will see substantially less noise, but also be limited to the traffic that has traversed the border. The decision on whether to place the sensor inside versus outside the border will typically depend on the defenders' tolerance for noise (alert fatigue), maturity, and their ability to operationalize the additional intelligence gained from the scan data.

2.2.4. *Cloud, Mobile, and Internet of Things*

Cloud computing and mobile devices reduce an organization's control over its network architecture, which adds complication. The internet of things adds another layer of complexity by incorporating physical systems and effects. While the CyDef Model can likely be extended to include these cases, additional development is necessary. As such, these are considered out-of-scope.

2.2.5. *Notes on the "Best" Location*

The purpose of defining the different locations above is to highlight the effect that location has on a CM's operation, scope, and requirements with regards to prevention, detection, and

response. These relative costs/benefits of each location should be taken into account when designing defenses.

For example, CMs deployed at the host have relatively low throughput and availability requirements, and access to host-specific data. This makes it possible for defenders to leverage fairly complex host-specific detection mechanisms. The down-side of host-deployed CMs is that their upkeep typically doesn't scale well, because there are many hosts on the network. Also, CMs at the host level will require a centralized reporting system for defenders to gain situational awareness, which is added effort.

On the flip side, CMs deployed at the border have relatively high throughput and availability requirements, and little or no access to host-specific data. This means that the CMs need to be limited to relatively simple detection rules that can be processed very quickly to handle the volume, velocity, and variety of data passing through the border. These CMs also do not have insight into data flowing within the network. The up-side of border-deployed CMs is that they scale well, because by design, they use a small number of devices. Also, these CMs do not typically need an extra reporting system, because they already offer a network-wide vantage point.

In the middle, CMs deployed at the intranet level have relatively moderate throughput and availability requirements, with some access to host-specific data. These CMs also have access to both data that traverses the network border, and internal network traffic, which offers a perspective not captured at either the host or the border. CMs deployed at this location must be configured to offer a reasonable tradeoff between throughput and availability requirements, and fidelity of information processed.

As will be discussed in Section 3, a “deep” defense needs to include CMs applied at all three locations, in order to best leverage the relative strengths of each.

2.3. Countermeasure (CM) Nomenclature

It is useful to have a systematic nomenclature for describing, at the conceptual level, what a CM does (e.g., what “action(s)” it takes and when). While this may not show up explicitly in the CyDef chart that will be discussed later, this nomenclature is essential for preliminary discussions in which stakeholders define possible CM options. Currently, many CMs are named in ways only somewhat descriptive of what they actually do, a name can be used to ambiguously describe more than one CM, and multiple names can be used to refer to the same CM. This can make it challenging for a security expert or an operations expert to convey to a decision-maker what a specific CM implementation does.

For example, most operations and security folks know that a firewall is a CM that inspects packet headers, and then either passes or blocks packets based on whether or not information in the packet header appears in the firewall’s blacklist. However, the name “firewall” itself is not particularly descriptive of what the CM is doing; in fact, the name derives from steam powered vehicles, where the firewall was a literal wall that separated the driver from the fire heating the boiler. The term is also used to describe the literal wall that separates a driver from the engine in a car, the engine compartment from the cockpit in a plane, and prevents fires from spreading across a building. So while the name makes it clear that the CM protects the user from something dangerous, it says absolutely nothing about what the CM itself does.

This unclear nomenclature is common in cybersecurity, and is compounded by the fact that for any CM name, it may be describing a general algorithm, a specific implementation of the algorithm, or a product that employs that technique. In addition, there are frequently many variations on a CM that sometimes results in a new CM name, and sometimes does not. Discussions between experts in cybersecurity can be muddled, which is a clear flag that nomenclature is an issue.

To provide a more systematic set of descriptors, we provide the following nomenclature: actions (organized by defense element), rules for when to apply the action, and variations on applying those actions and rules.

2.3.1. *Actions by Defense Element*

At the most basic level, CMs can be described in terms of the defense element to which they apply (**bold italic text**), the action they take (**bold text**), and the thing that the CM applies the action to. The actions are organized hierarchically.

For example, a specific firewall can be described as “packet blocking on IP traffic based on a blacklist.” This description of the CM is significantly more precise. Illustrations and examples for the Prevention actions are given in Table 1 and Table 2.

- *Prevention*

- **Pass:** Allow the packet to reach its destination, unaltered.
 - **Delay:** Artificially increase the time it takes a packet to reach its destination.
 - **Rate-Limit:** Limit the rate at which packets are allowed to pass.
 - **Tag:** Add a tag (or mark) to the packet without altering packet contents.
- **(Full) Block:** Prevent packets from reaching their destination.
 - **Drop:** Delete the packet/end the session.
 - **Redirect:** Change the destination of the packet/session.
 - **Substitute:** Impersonate the intended target.
- **(Partial) Block:** Prevent part of a packet from reaching its destination.
 - **Filter:** Drop only certain parts of the session.
 - **Modify:** Alter some aspect of the packet/session contents.
- **Inject:** Insert a packet, as if it had been sent.
- **Notify:** Return a notification to the sender (typically done in addition to one of the other actions noted above).

- *Detection*

- **Collect:** Manually record relevant data (content) and metadata (context).
- **Log:** Regularly and systematically record events.
- **Alert:** Actively get the attention of a defender when an event occurs.
- **Report:** Periodically provide a summary of certain aspects of the system.
- **Detect:** Use an indicator list to make a binary decision.
- **Judge:** Use reputational data, historical data, and/or algorithmic analytics to make a graded decision.
- **Discover:** Find new ways to detect and/or judge (e.g., hunting parties).
- **Attribute:** Determine the identity of the other party.

- *Response*

- **Scope:** Gain an understanding of the scope of the intrusion.
- **Log Forensic Data:** Systematically record forensics data.
- **Mitigate:** Minimize the possibility of additional damage.
- **Remediate:** Identify and clean all machines affected by the attack.
- **Eradicate:** Identify and close the attacker's point of ingress; fix the vulnerabilities/issue(s) that caused/enabled the incident.
- **Elevated Monitoring:** Allocate additional resources to provide extra oversight, typically focused on a subset of the network.

Table 1: Countermeasure Actions and Definitions

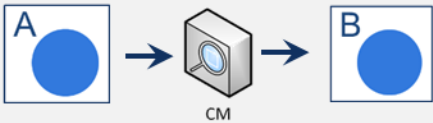
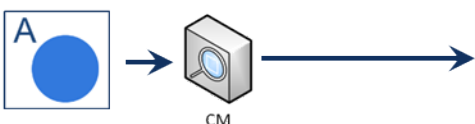
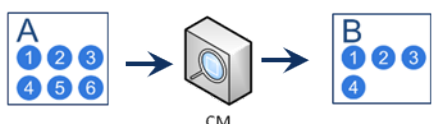
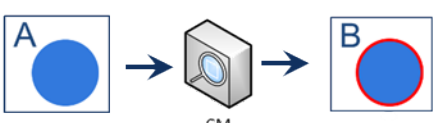


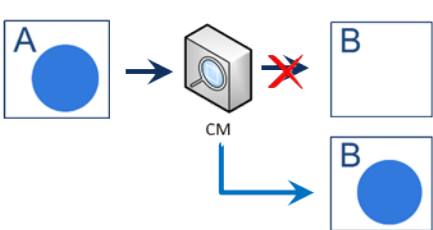
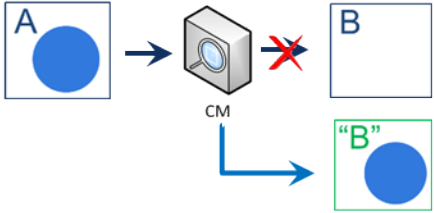
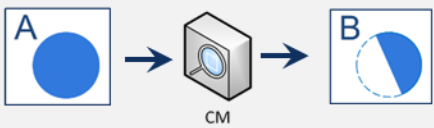
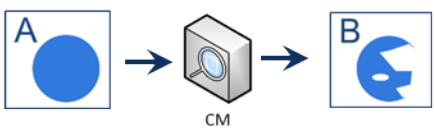
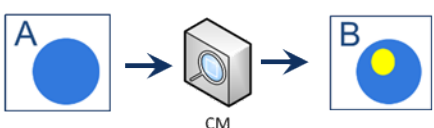


CM Action	Definition /Example
Pass 	Send a packet/establish a session Retrieving a webpage
Delay 	Artificially increase the time it takes a packet to reach its destination Network Tarpitting
Rate-Limit 	Restrict the number of packets passed per period of time.
Tag 	Add a tag (or mark) to the packet without altering packet contents.
(Full) Block 	Prevent a packet from reaching its destination. Packet Filtering
Drop 	Delete the packet/end the session. Packet Filtering
Redirect 	Change the destination of the packet/session. DNS Sinkholing

Table 2: Countermeasure Actions and Definitions, continued.

CM Action (continued)	Definition /Example
<p>Substitute</p> 	<p>Impersonate the intended target.</p>
<p>(Partial) Block</p> 	<p>Prevent only part of a packet/session from reaching its destination.</p>
<p>Filter</p> 	<p>Drop only certain parts of the packet/session. Web Content Filtering</p>
<p>Modify</p> 	<p>Alter some aspect of the packet/session.</p>
<p>Inject</p> 	<p>Insert a packet, as if it had been sent.</p>
<p>Notify</p> 	<p>Return a notification to the sender. Email Greylisting</p>

2.3.2. **Prevention Action Rules**

Prevention actions are typically triggered by a rule. Three common action rules are:

- **Blacklist:** maintain a list of indicators for “known bad” activity. Block any traffic that has indicators that appear on this list; otherwise, allow all other traffic to pass. This rule assumes that most traffic is legitimate.
- **Whitelist:** maintain a list of “known good” indicators. Allow any traffic that has indicators that appear on this list to pass; otherwise, block all other traffic. This rule assumes that most traffic is not legitimate.
- **Greylist:** maintain a list for what is “usual”. Temporarily block any traffic that is not on the list, but allow it if it meets set criteria for being categorized as “usual”. This rule is intended to be a middle ground between blacklists and whitelists.

2.3.3. **Variations on Applying Actions**

Different strategies could potentially leverage variations of the above actions based on *when* the action is applied. Below are some basic variations that can be applied to any of the actions and rules above.

- **Always:** Always apply the action when an indicator detects an issue.
- **Random:** Apply the action on a randomly-selected subset of cases where an indicator detects an issue.
- **Event-Based:** Apply the action if an external event or set of circumstances is fulfilled in addition to an indicator detecting an issue.
- **Temporary:** Temporarily apply the action for a set period of time.

In addition, different strategies could leverage variations of *how* the action is applied. Below are two common variations that can be applied to the actions and rules above.

- **Inline (active):** The CM sits between the sender and receiver, and operates on the traffic in real time. This provides real-time protections, but can potentially introduce issues into the system: for example, if an inline CM is taken down, the network behind it may experience a denial-of-service.
- **Out-of-line (passive):** The CM operates on a copy of the traffic, not in real time. This adds a slight delay between the CM acting on something it detects; however, this method prevents a denial-of-service if the CM is taken down.

This page is intentionally left blank.

3. CYBER DEFENSE MODEL COMPONENTS

This section includes the three sub-models that comprise the basis for the CyDef Model: the Cyber Attack Phases, the Pain Scale, and the Coverage Metric. These three scores can be estimated for any countermeasure (CM) that is being judged.

3.1. Cyber Attack Phases (CAPs)

The Cyber Attack Phase (CAP) model describes an attacker's general workflow by defining a series of steps that a CM can potentially inhibit. As shown in Figure 3, attacks proceed from left to right when successful. When attackers fail in one phase, they typically return to earlier phases and continue trying to move rightwards until they are successful.

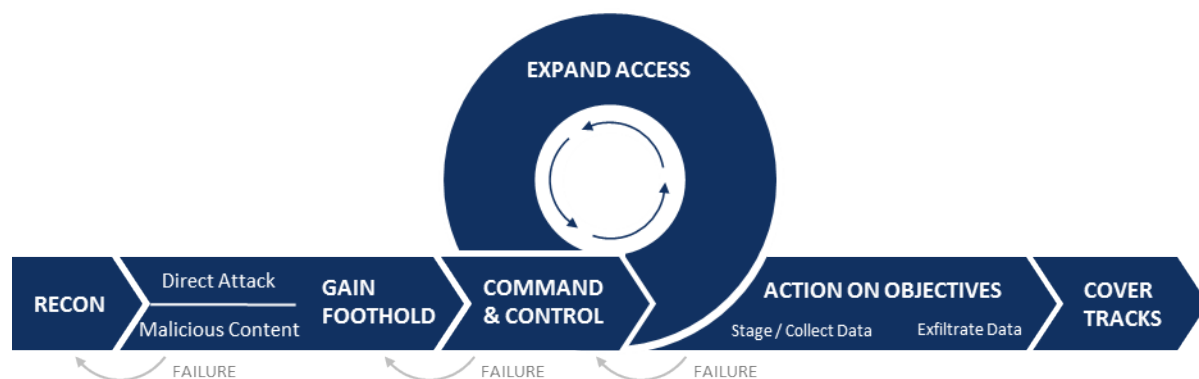


Figure 3: The Cyber Attack Phases (CAP), which shows an attacker's general workflow in terms of a series of steps that a defender can potentially inhibit.

It is important for defenders to develop a deep defense that thwarts threats across all phases, because no cyber defense is absolute. Later-phase countermeasures are particularly important for defenders to detect and efficiently respond to advanced adversaries.

The CAPs were inspired by Lockheed Martin's Cyber Kill Chain® [1]; however, the CAPs focus on phases that defenders can inhibit, which provides more-actionable information.

The individual phases are detailed below.

1. **Reconnaissance:** Attackers gather information about the network. This first phase is conducted from outside the network.
2. **Gain Foothold:** Attackers attempt to gain control of a host via:
 - a. **Direct Attack:** Hacking into a network resource that is directly accessible by the outside world
 - b. **Malicious Content:** Tricking users within the network into interacting with malicious code.
3. **Command & Control (C2):** Attackers establish a connection link to the host they control. They install tools to carry out the next phase, and now have in-network visibility.







4. **Expand Access:** Optional. Attackers seek to gain control of additional hosts, repeating phases 1-3 from within the network. This helps attackers establish persistence, and/or search for specific data. Sophisticated attackers may download different tools onto different hosts to increase persistence.
5. **Action on Objectives:** Attackers fulfill their objectives. Data exfiltration is shown here, though objectives for other data-based attacks (e.g. modification or deletion) also apply.
 - a. **Stage/Collect Data:** Attackers first aggregate the data in one location and prepare it for exfiltration, typically by compressing and encrypting it in chunks.
 - b. **Exfiltrate:** Attackers then move the data out of the network.
6. **Cover Tracks:** Sophisticated attackers cover their tracks by wiping their tools and camouflaging their presence on the systems they have touched.

3.2. The Pain Scale

The Pain Scale provides another axis of information in the CyDef Model. Strategically, a CM's score on the Pain Scale roughly translates to the level of difficulty that an attacker will face in attempting to directly circumvent that CM. CMs with a higher Pain score require an attacker to invest more time, effort, and/or resources to circumvent.

The Pain Scale is based on David Bianco's "Pyramid of Pain" [2], updated to account for the roughly logarithmic increase in pain for each step upwards. The levels are in fact ordinal; however, the model presented here provides a sufficient level of fidelity for the purpose at hand. The scores used for the pain score in this version of the model were generated by subject matter experts. Future versions of this model will establish a systematic set of metrics for calculating the "pain" associated with a given CM.

Table 3: The Pain Scale

	PAIN ^[3]	BIANCO'S EXAMPLE ^[2]	INTERPRETATION
100		Tactics, Techniques, & Procedures (TTPs)	Requires a change in attacker's fundamental workflow and strategy – tough to do.
		Tools	Requires attacker to invest in a new tool for future attacks – this is considered challenging.
10		Network Artifacts Host Artifacts	Requires attacker to change its tools or behaviors to leverage different artifacts (observables) – doable, but annoying.
		Domain Names	Requires attacker to change the domain (or subdomain) used in the attack – simple, but requires some effort.
		IP Addresses	Requires attacker to change the IP used in the attack – easy to do.
1		Hash Values	Requires the attacker to change the hash value of the malicious file – trivially simple to do.

3.3. Coverage Metric

The “attack surface” of a system represents the space of potential options an attacker has for attacking the network. For any given CM, it is useful to know whether it provides a solution that covers much of the attack surface, or if it blocks only a very specific class of attacks.

“Coverage” indicates the rough proportion of the attack surface that can be covered by a CM, based on reasonable assumptions about its implementation. Note that these assumptions and implementation requirements should be captured along with the coverage score, to ensure that different subject matter experts (SMEs) are using similar mental models for this metric.

Coverage is shown as a range of color shades in the CyDef Model, with darker CMs offering a higher level of coverage.



Figure 4: Coverage Metric

Conceptually, this translates to Figure 5. Higher-coverage CMs provide more-comprehensive protection of the attack surface, while lower-coverage CMs apply to a smaller proportion of the attack surface.

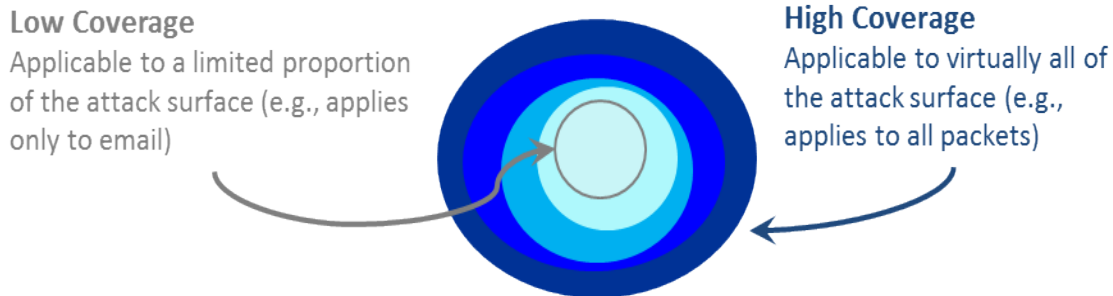


Figure 5: Conceptual diagram for the Coverage Metric

Depending on the organization's threat landscape, some CMs with lower coverage may need to be prioritized over CMs with higher coverage in order to address certain high-consequence threats.

The coverage metric will be most powerful when calculated for the system of CMs at large. When calculating the coverage metric for a set of CMs, a deep understanding of how the individual CMs are configured, architected, and deployed is required, because the exact implementation of a CM will vastly affect its effectiveness: two CMs that cover the same CAP may or may not increase the coverage of the overall system.

Additional research is necessary to determine how to combine the coverage scores of individual CMs into a global coverage score, how to automatically and systematically calculate this metric from network data, and how to leverage this metric for subtler changes, such as architectural changes.

4. THE CYBER DEFENSE (CYDEF) MODEL

The CyDef Model is represented by the CyDef chart, a simple visual representation for a CM that shows what Cyber Attack Phases (CAPs) it inhibits, and at what pain and coverage levels. The CyDef chart shows CAPs along the horizontal axis. A CM or system of CMs is represented by markers (solid squares) above each CAP that is addressed. The vertical position of each marker indicates the pain score for that CM in addressing the associated CAP, and the marker color becomes darker as its coverage increases with respect to the attack surface.

The example below shows the CyDef chart for Packet Filtering (i.e., a basic firewall that uses a blacklist and blocks all blacklisted traffic). For each CAP, the Packet Filtering CM was given a score according to how much pain it inflicted on an attacker and how much of the attack surface it covers. Because this firewall uses only hash and IP values in its blacklist, its pain score is relatively low; however, because it can be set to analyze every packet that flows through it, the CM has a high coverage score.

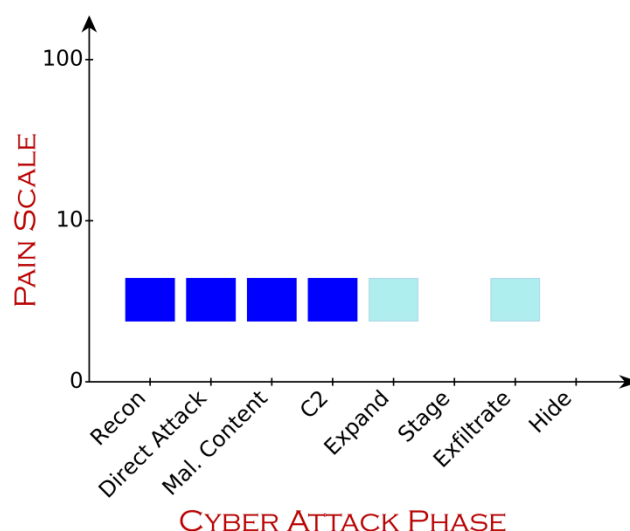


Figure 6: An example CyDef chart for packet filtering, a very common CM.

The CyDef chart can be generated for either a single CM, or for a group of CMs (e.g., for all CMs currently in use in the network). This provides a simple and flexible way for decision-makers to visually assess their organization's portfolio of defenses and to understand the technical return on investing in a new CM.

With the CyDef chart, as shown in Figure 7, it becomes immediately obvious if a new CM will provide additional “defense in depth” capabilities, or if it will “raise the bar” for the organization's network defense capabilities.

- **Defense in depth:** A deep defense offers comprehensive coverage of every CAP (and spans all locations), and is visually obvious in the CyDef chart, because a deeper defense results in a longer “depth” line in the chart.

- **Raising the bar:** A higher bar forces attackers to put in more effort to attack the system, and eventually drives them away from attacking the organization, in search of easier targets. In the CyDef chart, this literally shows up as a higher bar (i.e. higher pain).

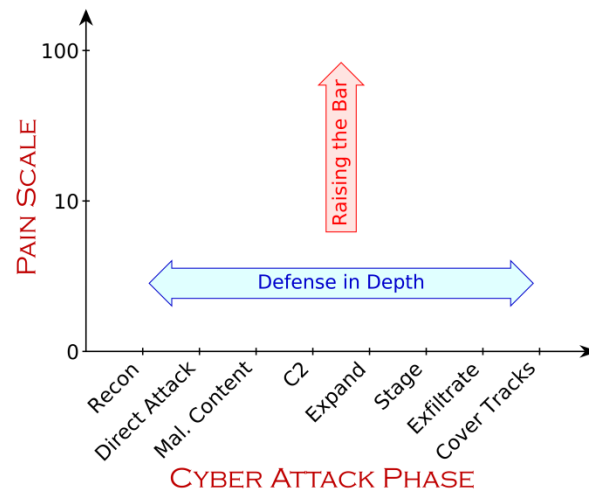


Figure 7: The CyDef chart, which displays a CM's applicable CAPs, with Pain and Coverage scores for each CAP.

Systematically laying out CM defenses in this way makes capability gaps and the potential return-on-investment of a new CM more obvious.

4.1. The CyDef Chart as a Decision Aid

The CyDef chart can aid in technical assessments and investment decisions: by overlaying the CyDef charts of proposed CMs over a CyDef chart for the organization's current portfolio of CMs, decision-makers can visualize gaps in current system capabilities and assess the expected gain in security from proposed CMs.

Ultimately, the “best” option will depend on the specifics of the deciding organization, because the CyDef chart is intended to enable and facilitate productive conversations between decision-makers, implementers, and stakeholders. The CyDef chart provides a high-level intuitive view, but does not itself provide answers.

As a note, there is nearly always a tradeoff between security and performance. The CyDef Model helps decision-makers quickly narrow their focus to a few promising CMs. However, because the CyDef model only shows effects on security, decision-makers should explicitly discuss the effects that any proposed CM may have on performance before making a final decision.

4.1.1. Example: CM Investment Decision

Suppose a decision-maker is tasked with picking a new CM to add to a system. The CyDef chart in Figure 8 succinctly summarizes the coverage offered by the existing system (blue) and the two proposed CMs. As one can clearly see in the chart, CM #1 (green) increases the number of CAPs

that are protected, but at a relatively low level; whereas CM #2 (purple) offers an improved level of protection in two phases that are already covered.

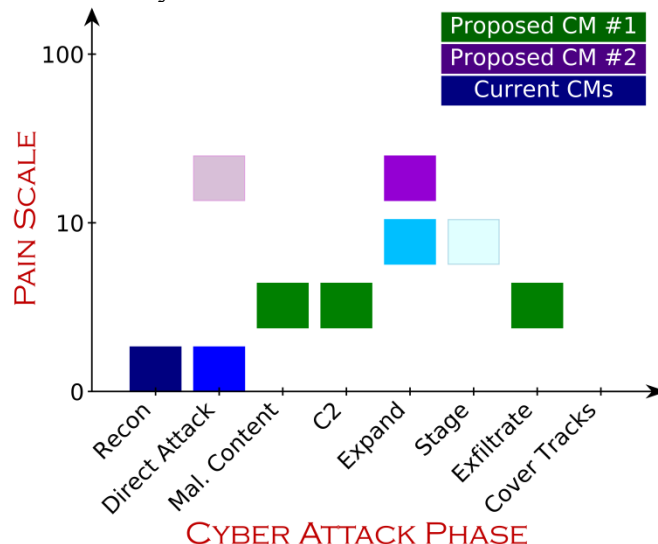


Figure 8: CyDef chart an example decision.

So, which CM is a smarter investment? In reality, the “better” CM to invest in will depend on the goals of the organization.

For example, for an internet-connected network, CM #1 is likely a better choice because it fills critical gaps in the current set of defenses, providing protection against adversaries in the Malicious Content, C2, and Exfiltration CAPs. In contrast, CM #2 provides a higher level of protection in CAPs that already have at least some coverage, so its relative benefit may be lower.

Conversely, for an air-gapped network, CM #2 is likely a much better choice, because additional CMs are not needed for the Malicious Content, C2, and Exfiltration CAPs, because those are covered by the air gap. For this situation, CM #2 is the better choice, because it increases protection in the Direct Attack and Expand CAPs, which are more critical to the air-gapped network.

The CyDef chart did not provide any answers in this example. Instead, it clearly outlined the current state of the organization’s defenses and highlighted the potential benefit of each new CM option. Additional context on the system then made the better option more obvious.

As a note: once the “best” CM is selected, the decision-maker’s next step should be to investigate whether the selected CM is compatible with the organization’s performance needs. This ensures that answers like “scissors are the best countermeasure” will not arise from the analysis.

This simple example demonstrates how the CyDef chart can be used to assess an organization’s cybersecurity posture, highlight gaps, and make informed strategic decisions on CM investments.

This page is intentionally left blank.

5. CONCLUSIONS & NEXT STEPS

This paper provides a series of foundational models and systems of nomenclature for discussing cybersecurity countermeasures (CMs) and CM effectiveness, culminating in the Cyber Defense (CyDef) model. This provides a systematic way to organize and visualize CM information so that an organization can gain a high level and more intuitive view of its current defensive capabilities, more easily identify gaps, understand how any new CM might enhance existing defenses, compare and prioritize options, and ultimately make smarter and more strategic cybersecurity investment decisions.

Additional research will be necessary to develop this model into one that can be linked to operations data, and/or used for subtler decisions, such as architectural design. Future work will also provide more detail on the individual components of this model, and may leverage other existing metrics, such as the MITRE ATT&CK model.

This page is intentionally left blank.

6. REFERENCES

1. Lockheed Martin, *The Cyber Kill Chain*, <http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>, 2017. Accessed 22 May 2017.
2. David Bianco, *The Pyramid of Pain*, <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>, 17 January 2014. Accessed 22 May 2017.
3. Allie Brosch, *A More Accurate Pain Scale*, Hyperbole and a Half, <https://brainhatesme.com/2013/05/11/a-more-accurate-pain-scale-hyperbole-and-a-half/>, 11 May 2013. Accessed 22 May 2017.

This page is intentionally left blank.

DISTRIBUTION

1	MS0899	Technical Library	9536 (electronic copy)
---	--------	-------------------	------------------------

